The Management Committee of

Herons Dale Primary School

have adopted the following policy:

Online Safety Policy

Ratified by Governors: Oct 18

Review Date: Oct 2020

On Line Safety at Herons Dale School

At Herons Dale School we understand that technology can have an important role to play in overcoming barriers and supporting learning. At Herons Dale we are also mindful that some children may be vulnerable when using technology because they may have difficulty in social understanding.

We take Internet Safety very seriously and see it as our duty to keep our pupils safe whilst using technology in school and at home.

This policy covers 4 main areas; **children's safety**, **staff's responsibilities, network managers and senior leaders** and **support for parents.**

Children's Safety

At Herons Dale School pupils can use the internet in educational, creative, empowering and fun ways.

Computers are used to support learning across all curriculum areas as they make information accessible, use simplified language and emotions, present video clips to consolidate learning, offer games to embed learning and give repetition to support children who take longer to learn new things

However, some of our pupils may be vulnerable to on line safety risks.

Some children may not understand terminology due to language delays or disorders.
Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
Some children with SEN or disabilities may be vulnerable to being bullied through the internet, or not recognize that they are being bullied.
Some children may not appreciate how their own online behavior may be seen by someone else as bullying.
Some of our children may not be aware of the age restrictions on the games they play when out of school

Strategies for safe internet use

The school's Network is presently managed by the school business manager in conjunction with an External Contractor – TC-IT Services Limited. The email, Web Filtering and security are managed by Atomwide.

Weekly meetings take place with Office Manager and External contractor. During this meeting any issues with the Network and on-line safety issues are dealt with. Any misuse / attempted misuse will be reported to the E-Safety/OnLine Safety Co-ordinator / Headteacher / Computing Co-ordinator for investigation / action / sanction

Webscreen 2, provided by Atomwide is a highly effective monitoring system which identifies cyberbullying and other safeguarding concerns, and is used in school as part of the Local Authority's support for On-Line Safety. All internet activity is logged and reports can be generated by nominated contacts within the school.

Safety and Responsibilities for Staff

All staff are required to read and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the work place.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone. I will not log on for another person.
- I will not allow unauthorised individuals to access E-Mail / Internet / Intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook.
- I will only use the approved, secure E-Mail system(s) for any school business.
- I will only use the approved school E-Mail, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- At any time I will not use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or pupils.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will ensure that any 'loaned' equipment is up-to-date, with the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personally owned digital cameras or camera/mobile phones for taking and transferring images/videos of pupils or staff without permission and will not store images at home.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's On Line Safety curriculum into my teaching.
- I understand that all Internet usage / and network usage is monitored and that monitoring data could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
    - OnLine Safety training will be provided to all members of staff once a year and it is each person's responsibility to attend this session. These sessions will be arranged by the ICT Coordinator and be held in term 1.

At Herons Dale School staff make sure that pupils they are responsible for are using the Internet safely. High risk students will be highlighted and staff will be made aware of these students.
On Line Safety posters with symbol-support are displayed where appropriate.
The school council are included in online safety matters where appropriate
Online safety day is celebrated and assemblies are provided
Books are available for parents to borrow when talking about on line safety at home

Unsuitable / inappropriate activities

The activities listed below would be inappropriate in a school context and staff should not engage in these activities in school or outside school when using school equipment or systems.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity,
- computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by West Sussex and / or the school

- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial
    - /personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling
- Use of social networking sites

Responding to incidents of misuse

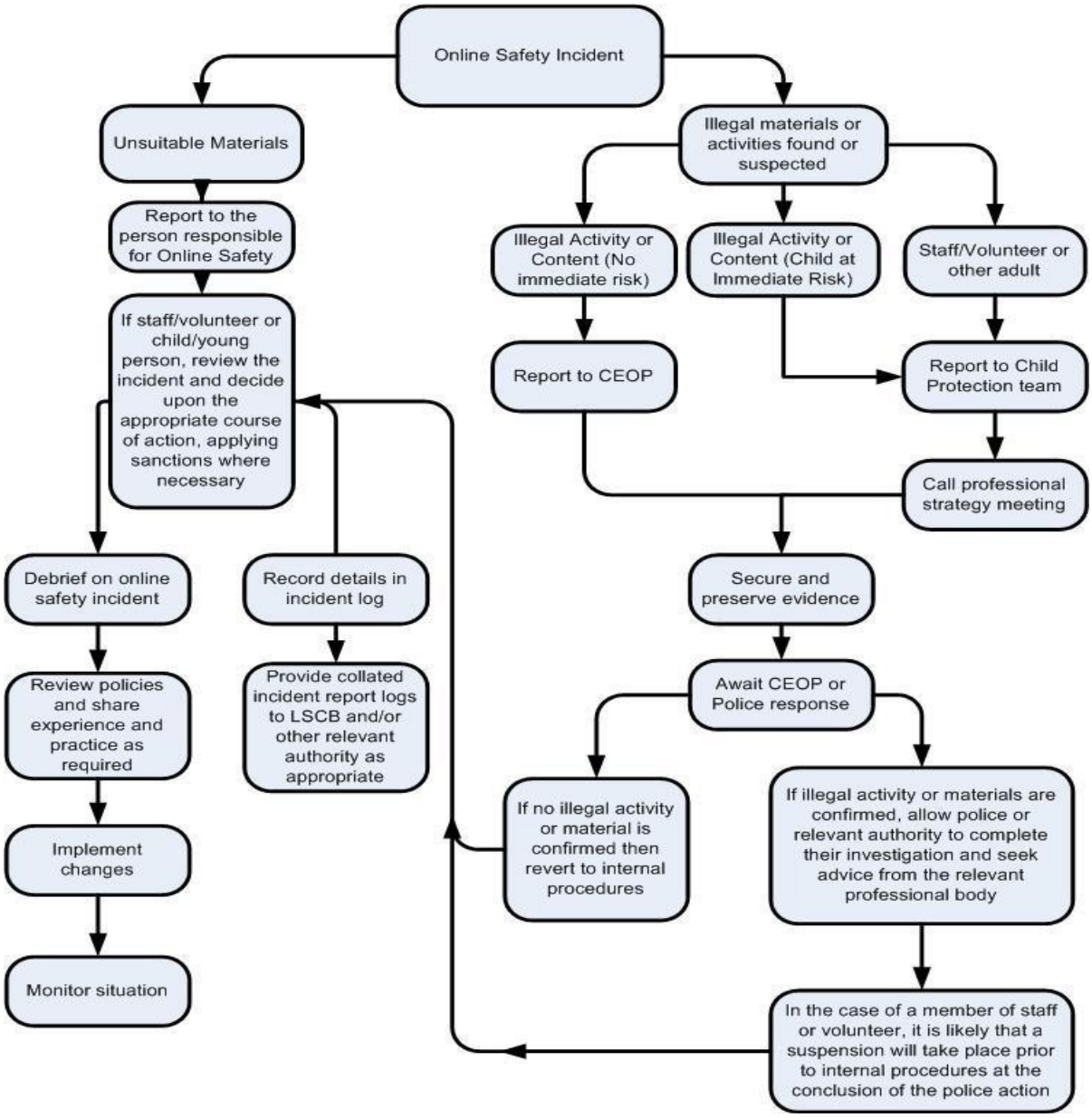
It is likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

There may be times when infringements of the policy could take place, through careless or deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the flow chart – below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

Head Teacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher / Senior Leaders are responsible for ensuring that the staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

On Line Safety / Child Protection Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Attends relevant meeting
- Reports regularly to Senior Leadership Team
- **Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:**
- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Network Manager / Technical staff:

The Network Manager and computing Co-ordinator are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the on line safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E- Safety Policy and guidance
- that Atomwide is informed of issues relating to the filtering applied
- that he / she keeps up to date with e-safety technical information in order to
- effectively carry out their on-line safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse
- can be reported to the On-Line Safety Co-ordinator / Headteacher / computing Co-ordinator for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed in school policies
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.
The parents will be invited to On-line Safety sessions which will be held in school once a year.
The school web site will have information regarding On- Line Safety for parents / carers and young people.

Although some of our pupils are unable to access the Internet some pupils are able to use the Internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.
No child is able to access the Internet in school without their parents giving permission to do so. This consent form is filled in when the child starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.
All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the computing curriculum.

No child may appear on the Web Site without their parent/carers consent, the consent form is completed when the child starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.